**Steps and commands to conduct the attack:**

1. First, we need to have VMware or Virtual Box in our systems.
2. After installing any one of the virtual machine operators mentioned above. Now its time to install Kali Linux and Metasploit able 2.
3. After successfully installing both operating systems. We must do some configurations. For Eg: need to change the network adapter from NAT to Bridged Adapter.
4. Need to check the net mask of kali Linux by the command ***“ifconfig”***. So, we can allot new Ip address with same net mask to Metasploit able 2.
5. To Allot new Ip address in Metasploit able 2 we will use the following command ***“sudo ifconfig eth0 <Ip Address you want to add> netmask <netmask of kali Linux>”***
6. We will check that is the Ip address allotted or not by the command ***“ifconfig”***
7. Will also check it by connecting it from kali Linux by the command ***“ping <Ip Address>”*** by also applying ctrl+d to halt the process if successfully connected.
8. Now it’s time to open the browser and browse the Ip address allotted.
9. Click on the Muttilidae. Select OWASP Top 10 -> A1 – Injection -> SQLi - Extract Data -> User Info.
10. Now we must start the Burp suite (which is already installed on kali Linux) and start burp process with default settings.
11. It’s time to change the proxy settings of our browser. We must enter proxy ***“127.0.01”*** with port No as ***“8080”*** and just make sure intercept is on.
12. Now try to login with any credentials you want and when intercept catches anything just save it as a txt file
13. Now once we have the txt file. We must run this command ***“sqlmap -r <directory of the txt extracted file> --dbs”***
14. We will use the default option which is 0. Enter 0 which will fetch the backend dbs of MySql
15. To access any database table, use the following command:  
    ***“sqlmap -r <directory of the txt extracted file> -D <database name> --tables”*** again select the default option of 0.
16. Now if you want to fetch the table data, use the following command:  
    ***“sqlmap -r <directory of the txt extracted file> -D <database name> -T <table name> --dump”*** again select the default option of 0.